FortiOS - Release Notes

Version 6.2.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 21, 2019
FortiOS 6.2.2 Release Notes
01-622-577858-20191021

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-10-09	Initial release.
2019-10-10	Added 551119 to *Resolved Issues*. Added commands to the Previous releases column in *Changes in CLI defaults SSH* and *SSL VPN* sections.
2019-10-16	Added 589234 to *Known Issues*. Added item to *Changes in default behavior > System*.
2019-10-18	Added 569310 to *Resolved Issues*.
2019-10-21	Added 535099, 572350, 586301, 586604, 588262, 588436, and 588908 to *Known Issues*. Added 546964, 550056, 560438, and 570575 to *Resolved Issues*. Deleted 570686, 576288, and 579400 from *Resolved Issues*.

Introduction and supported models

This guide provides release information for FortiOS 6.2.2 build 1010.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.2 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-POE, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-61E
FortiGate Rugged	FGR-30D, FGR-35D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.2.2 images are delivered on request and are not available on the Beta portal.

Special branch supported models

The following models are released on a special branch of FortiOS 6.2.2. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1010.

FGR-90D	is released on build 5335.

Special notices

Common vulnerabilities and exposures

FortiOS 6.2.1 is no longer vulnerable to the issue described in the following link - https://fortiguard.com/psirt/FG-IR-19-144.

New Fortinet cloud services

FortiOS 6.2.0 introduced several new cloud-based services listed below. The new services require updates to FortiCare and Fortinet's FortinetOne single sign-on (SSO) service. These updates will be available by mid-Q2 2019.

- Overlay Controller VPN
- FortiGuard Cloud-Assist SD-WAN Interface Bandwidth Monitoring
- FortiManager Cloud
- FortiAnalyzer Cloud

FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate model:

- FGR-30D
- FGR-35D
- FGT-30E
- FGT-30E-MI

- FGT-30E-MN
- FGT-50E
- FGT-51E
- FGT-52E
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E
- FWF-50E-2R
- FWF-51E

FortiGate hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D does not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

NP4lite platforms

FortiOS 6.2 and later does not support NP4lite platforms.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

Mobile token authentication

Mobile token authentication does not work for SSL VPN on SOC3 platforms.

Affected models include FG-60E, FG-60E-POE, FG-61E, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-100E, FG-100EF, FG-101E, FG-140E, FWF-60E, FWF-61E.

Changes in default behavior

AntiVirus

- In previous releases, the scan mode controls which features are displayed based on their compatibility with proxy and flow's `[quick | full]` mode (now `[default | legacy]`).
  This release disregards this behavior, making antivirus profile scan-mode agnostic. This means that all AV options are displayed regardless of the AV profile's scan-mode setting. Enforcement is handled by the kernel based on the firewall policy using AV. Unsupported AV features do not take effect if inspection mode is proxy or flow.
- In this release, AntiVirus can do SSH inspection.

FOC

`apn` option under `apn-shaper` now accepts multiple `apn` or `apngroup`.

Previous releases	6.2.2 release

`config gtp apn`
`  edit "apn1"`
`  set apn "internet"`
`  next`
`  edit "apn2"`
`  set apn "intranet"`
`  next`
`end`
 	
`config gtp apngrp`
`  edit "apngrp1"`
`  set member "apn1"`
`  next`
`end`
 	
`config gtp apn-shaper`
`  edit 1`
`  next`
`end`
	`config gtp apn`
	`  edit "apn1"`
	`  set apn "internet"`
	`  next`
	`  edit "apn2"`
	`  set apn "intranet"`
	`  next`
	`end`
	
	`config gtp apngrp`
	`  edit "apngrp1"`
	`  set member "apn1"`
	`  next`
	`end`
	
	`config gtp apn-shaper`
	`  edit 1`
	`  set apn "apn2" "apngrp1" <==changed`
	`  next`
	`end`

FortiSwitch Controller

- FortiLink interface is on by default on FortiGate E series platform.
  - On FG-100E and higher, create an empty FortiLink aggregate interface (fortilink) by default. If aggregate interface is not supported, create a hardware switch interface instead.
  - For FortiGate models below FG-100E, create an empty FortiLink hardware switch interface (fortilink) by default. If hardware switch interface is not supported, create aggregate interface instead.
- When the FortiLink interface is enabled, CLI displays an error message when trying to change the FortiGate to TP mode.

Firewall

- Only IP and Protocol are matched and source port is ignored when ISDB is applied as source in policy.
- Internet-service-addition will overwrite default ports of internet-service ID if protocols are the same.
- Firewall policy supports `wildcard-fqdn` object with FQDN type.
- This release supports `srcaddr/dstaddr/internet-service/internet-service-src` negate in consolidated policy.
- All attributes for FABRIC_DEVICE object, except for IP address and type, can be modified from CLI but not from GUI.

Log & Report

- In previous releases, FortiGate only sends event log to FAZ-Cloud. In this release, FortiGate sends both event log and UTM log to FAZ-Cloud.

Switch

- Add VLAN switch feature to FG-300E and FG-301E.

System

- API user must have at least one trust host IP Address.
- Only show `diagnose sys nmi-watchdog` command on platforms that have "nmi" button.
- With mgmt interface set to dedicated to management, added three kinds of cases.
  - When no trust host is set, all IPv4 and IPv6 addresses have access.
  - When only IPv4 addresses are set to trust host, IPv6 address cannot log in.
  - When only IPv6 addresses are set to trust host, IPv4 address cannot log in.
- There is no mgmt option in GRE tunnel interface when it is set to dedicated to management.
- Allow VDOM admin to create loopback interface if no physical interface in VDOM.
- The `trust-ip` option in `config system interface` always override `trusthost` option in `config system admin`.
- When `vdom-dns` is disabled in non-management, the system DNS is used in the DHCP server by default.

Changes in CLI defaults

AntiVirus

Add SSH inspection. This is only compatible with proxy inspection.

Previous releases	6.2.2 release
config antivirus profile edit "profile_name" next end	config antivirus profile edit "profile_name" **config ssh <==added** **set options scan <==added** **unset archive-block <==added** **unset archive-log <==added** **set emulator enable <==added** **set outbreak-prevention disabled <==added** end next end

Endpoint Control

Add `fortiems-cloud` option under FSSO user.

Previous releases	6.2.2 release
config user fsso edit <name> next end	config user fsso edit <name> **set type fortiems-cloud <==added** next end

Add attribute `fortinetone-cloud-authentication` to endpoint control `fctems`.

Previous releases	6.2.2 release
config endpoint-control fctems edit <name> next end	config endpoint-control fctems edit <name> **set fortinetone-cloud-authentication [enable | disable] <==added** next end

Add `sub-second-sampling` under GTP.

Previous releases	6.2.2 release
config firewall gtp edit "gtpp" next end	config firewall gtp edit "gtpp" **set sub-second-sampling enable <==added** **set sub-second-interval 0.1 <==added** next end

Firewall

Add HTTPS as a type of health check for VIP load-balance monitor.

Previous releases	6.2.2 release
config firewall ldb-monitor edit [Monitor Name] set type ? ping PING health monitor. tcp TCP-connect health monitor. http HTTP-GET health monitor.	config firewall ldb-monitor edit [Monitor Name] set type ? ping PING health monitor. tcp TCP-connect health monitor. http HTTP-GET health monitor. **https HTTP-GET health monitor with SSL. <==added**

Remove `set type wildcard-fqdn` and `set wildcard-fqdn <string>` from firewall address.

Previous releases	6.2.2 release
config firewall address edit [Address] **set type wildcard-fqdn <==removed** **set wildcard-fqdn <string> <==removed** next end	config firewall address edit [Address] next end

Add CLI commands to support address and service negate in consolidated policy.

Previous releases	6.2.2 release
config firewall consolidated policy edit [Policy ID] next end	config firewall consolidated policy edit [Policy ID] **set srcaddr-negate [enable | disable] <==added** **set dstaddr-negate [enable | disable] <==added** **set service-negate [enable | disable] <==added**

Previous releases	6.2.2 release
	set internet-service-negate [enable | disable] <==added **set internet-service-src-negate [enable | disable] <==added** next end

Proxy

In protocol option profile, add `ssl-offloaded` command under each protocol.

Previous releases	6.2.2 release
config firewall profile-protocol-options edit ""default-clone"" config http end config ftp end config imap end config pop3 end config smtp end next end	config firewall profile-protocol-options edit ""default-clone"" config http **set ssl-offloaded no <==added** end config ftp **set ssl-offloaded no <==added** end config imap **set ssl-offloaded no <==added** end config pop3 **set ssl-offloaded no <==added** end config smtp **set ssl-offloaded no <==added** end next end

Traffic Shaping

Add a new global CLI table to define traffic classes. This is 's a mapping between `class-ID` and naming. `class-ID` from shaping-policy, shaping-profile, and traffic-shaper need to be data-sourced from this CLI table.

Previous releases	6.2.2 release
	config firewall traffic-class <==added **edit [Class-ID] <==added** **end <==added**

Log & Report

Add CLI allowing user to configure socket priority and maximum log rate per remote log device.

Similar setting apply to `config log fortiguard setting` and `config log syslogd setting`.

Previous releases	6.2.2 release
config log fortianalyzer setting end config log fortianalyzer override-setting end	config log fortianalyzer setting **set priority [default | low] <==added** **set max-log-rate [Log Rate, unit is MBps] <==added** end config log fortianalyzer override-setting **set priority [default | low] <==added** **set max-log-rate [Log Rate, unit is MBps] <==added** end

Add the test command option in CLI.

Previous releases	6.2.2 release
diag test application miglogd	**diag test application miglogd 40 <==added option "40"**

SSH

Add file transfer scan over SSH (SCP and SFTP).

Previous releases	6.2.2 release
config ssh-filter profile edit [Profile Name] set default-command-log disable next end	config ssh-filter profile edit [Profile Name] **set block x11 shell exec port-forward tun-forward sftp scp unknown <==added scp** **set log x11 shell exec port-forward tun-forward sftp scp unknown <==added scp** set default-command-log disable **config file-filter <==added** **set status enable <==added** **set log enable <==added** **set scan-archive-contents enable <==added** **config entries <==added** **edit [Entry] <==added** **set comment '' <==added** **set action block <==added** **set direction any <==added** **set password-protected any <==added** **set file-type "msoffice" <==added**

Previous releases	6.2.2 release
	next end end next end

SSL VPN

Remove `citrix` and `portforward` from `apptype` in the three entries in SSL VPN web bookmark.

Previous releases	6.2.2 release
conf vpn ssl web user-bookmark edit [Name] config bookmarks edit [Boormark Name] set apptype ? **citrix Citrix. <==removed** ftp FTP. **portforward Port Forward. <==removed** rdp RDP. sftp SFTP. smb SMB/CIFS. ssh SSH. telnet Telnet. vnc VNC. web HTTP/HTTPS. next end next end conf vpn ssl web user-group-bookmark edit [Name] config bookmarks edit [Boormark Name] set apptype ? **citrix Citrix. <==removed** ftp FTP. **portforward Port Forward. <==removed** rdp RDP. sftp SFTP. smb SMB/CIFS. ssh SSH.	conf vpn ssl web user-bookmark edit [Name] config bookmarks edit [Boormark Name] set apptype ? ftp FTP. rdp RDP. sftp SFTP. smb SMB/CIFS. ssh SSH. telnet Telnet. vnc VNC. web HTTP/HTTPS. next end next end conf vpn ssl web user-group-bookmark edit [Name] config bookmarks edit [Boormark Name] set apptype ? ftp FTP. rdp RDP. sftp SFTP. smb SMB/CIFS. ssh SSH. telnet Telnet. vnc VNC. web HTTP/HTTPS. next end

Previous releases	6.2.2 release
telnet Telnet. vnc VNC. web HTTP/HTTPS. next end next end conf vpn ssl web portal edit [Name] config bookmarks edit [Boormark Name] set apptype ? **citrix Citrix. <==removed** ftp FTP. **portforward Port Forward. <==removed** rdp RDP. sftp SFTP. smb SMB/CIFS. ssh SSH. telnet Telnet. vnc VNC. web HTTP/HTTPS. next end next end	next end conf vpn ssl web portal edit [Name] config bookmarks edit [Boormark Name] set apptype ? ftp FTP. rdp RDP. sftp SFTP. smb SMB/CIFS. ssh SSH. telnet Telnet. vnc VNC. web HTTP/HTTPS. next end next end

System

Add description in system security zones.

Previous releases	6.2.2 release
config system zone edit [Zone Name] next end	config system zone edit [Zone Name] **set description "" <==added** next end

Increase the maximum number of DNS servers supported in DHCP server from 3 to 4.

Previous releases	6.2.2 release
config system dhcp server edit [Server ID] set dns-server1 1.1.1.1 set dns-server2 2.2.2.2 set dns-server3 3.3.3.3 next end	config system dhcp server edit [Server ID] set dns-server1 1.1.1.1 set dns-server2 2.2.2.2 set dns-server3 3.3.3.3 **set dns-server4 4.4.4.4 <==added** next end

VM

Remove `vdom-mode multi-vdom` option for cloud-based ondemand FGT-VM.

Previous releases	6.2.2 release
config sys global set vdom-mode ? no-vdom Disable split/multiple VDOMs mode. split-vdom Enable split VDOMs mode. **multi-vdom Enable multiple VDOMs mode. <==removed** end	config sys global set vdom-mode ? no-vdom Disable split/multiple VDOMs mode. split-vdom Enable split VDOMs mode. end

Remove security rating from FGT_VMX and FGT_SVM.

Previous releases	6.2.2 release
diagnose security-rating version <==removed	

Enable CPU hot plug in kernel configuration.

Previous releases	6.2.2 release
	execute cpu show <==added Active CPU number: 1 Total CPU number: 8 **execute cpu add 1 <==added** Active CPU number: 2 Total CPU number: 8

Collect EIP from cloud-VMS (Azure, AWS, GCP, AliCloud, and OCI).

Previous releases	6.2.2 release
pcui-cloudinit-test # execute <?> config sys interface edit [Name] next end conf sys global **set sslvpn-cipher-hardware-acceleration <==removed** end	pcui-cloudinit-test # execute <?> **update-eip Update external IP. <==added** config sys interface edit [Name] **set eip <==added** next end conf sys global end

WiFi Controller

Add portal-type `external-auth` when `captive-portal` is enabled on local-bridge VAP.

Previous releases	6.2.2 release
config wireless-controller vap edit "wifi.fap.02" set ssid "bridge-captive" set local-bridging enable set security captive-portal set external-web "170.00.00.000/portal/index.php" set radius-server "peap" next end	config wireless-controller vap edit "wifi.fap.02" set ssid "bridge-captive" set local-bridging enable set security captive-portal **set portal-type external-auth <==added** set external-web "170.00.00.000/portal/index.php" set radius-server "peap" next end

Move `darrp-optimize` and `darrp-optimize-schedules` configurations from Global level to VDOM level.

Previous releases	6.2.2 release
### Global ### config wireless-controller timers **set darrp-optimize 86400 <==removed** **set darrp-optimize-schedules "default-darrp-optimize" <==removed** end	**### VDOM ###** config wireless-controller setting **set darrp-optimize 86400 <==added** **set darrp-optimize-schedules "default-darrp-optimize" <==added** end

Add `external-web-format` setting under `captive-portal` VAP when external portal is selected.

Previous releases	6.2.2 release
config wireless-controller vap edit guestwifi set ssid "GuestWiFi" set security captive-portal set external-web "http://170.00.00.000/portal/index.php" set selected-usergroups "Guest-group" set intra-vap-privacy enable set schedule "always" next end	config wireless-controller vap edit guestwifi set ssid "GuestWiFi" set security captive-portal set external-web "http://170.00.00.000/portal/index.php" set selected-usergroups "Guest-group" set intra-vap-privacy enable set schedule "always" **set external-web-format auto-detect** **<==added** next end

Add new WTP profiles `FAPU431F-default` and `FAPU433F-default`.

Previous releases	6.2.2 release
config wireless-controller wtp-profile edit [FAPU431F-default | FAPU433F-default] config platform end	config wireless-controller wtp-profile edit [FAPU431F-default | FAPU433F-default] config platform **set type [U431F | U433F] <==added** **set mode [dual-5G | single-5G] <==added** end
config wireless-controller wtp-profile edit [FAPU431F-default | FAPU433F-default] next end	config wireless-controller wtp-profile edit [FAPU431F-default | FAPU433F-default] **config radio-1 <==added** **set band 802.11ax-5G <==added** end **config radio-2 <==added** **set band 802.11ax-5G <==added** end **config radio-3 <==added** **set band 802.11n,g-only <==added** end next end
config wireless-controller vap edit [SSID name] next end	config wireless-controller vap edit [SSID name] **set high-efficiency enable <==added** **set target-wake-time enable <==added** next end

For DFS approved countries, add 160 MHz channel bonding support for FortiAP U421EV/U422EV/U423EV models.

Previous releases	6.2.2 release
config wireless-controller wtp-profile edit [FAPU421EV-default | FAPU422EV-default | FAPU423EV-default] config radio-2 set band 802.11ac end next end	config wireless-controller wtp-profile edit [FAPU421EV-default | FAPU422EV-default | FAPU423EV-default] config radio-2 set band 802.11ac **set channel-bonding 160MHz <==added** end next end

Add MPSK schedule that allows setting valid period for MPSK.

Previous releases	6.2.2 release
config wireless-controller vap edit [SSID Interface Name] set mpsk enable config mpsk-key edit [MPSK Entry Name] set passphrase 11111111 next end next end	config wireless-controller vap edit [SSID Interface Name] set mpsk enable config mpsk-key edit [MPSK Entry Name] set passphrase 11111111 **set mpsk-schedules "always" <==added** next end next end

Add GRE&L2TP support in WiFi.

Previous releases	6.2.2 release
config wireless-controller vap edit "80e_gre" set ssid "FOS-QA_Bruce_80e_gre" set local-bridging enable set vlanid 3135 next end	**config wireless-controller wag-profile <==added** **edit [Profile Name] <==added** end config wireless-controller vap edit "80e_gre" set ssid "FOS-QA_Bruce_80e_gre" set local-bridging enable set vlanid 3135 **set primary-wag-profile "tunnel" <==added** **set secondary-wag-profile "l2tp" <==added** next end

Changes in default values

AntiVirus

Change AV scan mode from `[quick | full]` to `[default | legacy]`. The default value is set to `default`.

Previous releases	6.2.2 release
config antivirus profile edit "profile_name" **set scan-mode [quick | full]** next end	config antivirus profile edit "profile_name" **set scan-mode [default | legacy] <==changed** next end

Log & Report

Change default value from `disable` to `enable` for some configuration options under `fortianalyzer-cloud filter`.

Previous releases	6.2.2 release
config log fortianalyzer-cloud filter set severity information set forward-traffic disable set local-traffic disable set multicast-traffic disable set sniffer-traffic disable set anomaly disable set voip disable set dlp-archive disable set filter '' set filter-type include end	config log fortianalyzer-cloud filter set severity information **set forward-traffic enable <==changed** **set local-traffic enable <==changed** **set multicast-traffic enable <==changed** **set sniffer-traffic enable <==changed** **set anomaly enable <==changed** **set voip enable <==changed** set dlp-archive disable set filter '' set filter-type include end

System

After creating a new VDOM, add default certificates for `ssl-cert` and `ssl-ca-cert` under `web-proxy` setting.

Previous releases	6.2.2 release
show web-proxy global config web-proxy global set ssl-cert '' set ssl-ca-cert '' set proxy-fqdn "default.fqdn" end	show web-proxy global config web-proxy global **set ssl-cert 'Fortinet_Factory' <==changed** **set ssl-ca-cert 'Fortinet_CA_SSL' <==changed** set proxy-fqdn "default.fqdn" end

WiFi Controller

Change default LLDP setting in `wtp-profile` from `disable` to `enable`.

Previous releases	6.2.2 release
config wireless-controller wtp-profile edit [FAP-Profile] set lldp disable end end	config wireless-controller wtp-profile edit [FAP-Profile] **set lldp enable <==changed** end end

The default `channel-utilization` setting in `wtp-profile` is changed from `disable` to `enable`.

Previous releases	6.2.2 release
config wireless-controller wtp-profile edit [FAP Profile Name] config radio-1 set channel-utilization disable end config radio-2 set channel-utilization disable end next end	config wireless-controller wtp-profile edit [FAP Profile Name] config radio-1 **set channel-utilization enable <==changed** end config radio-2 **set channel-utilization enable <==changed** end next end

Increase normal WTP capacity on high end FortiGates from 1024 to 2048.

Previous releases	6.2.2 release
FGT(1000, end) = 1024 -> 2048	FGT(1000, end) = 1024 -> 2048

Upgrade Information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- Mac-address-based policies – A new address type is introduced (Mac Address Range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.2.2 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.0
- FortiClient EMS 6.2.0
- FortiClient 6.2.0
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.9 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.2. When Security Fabric is enabled in FortiOS 6.2.2, all FortiGate devices must be running FortiOS 6.2.2.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.2 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.2.2 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)

- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 6.2.2 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.2 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.2.2, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.2.2.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

FortiView widgets have been rewritten in 6.2.2. FortiView widgets created in previous versions are deleted in the upgrade.

Product integration and support

The following table lists FortiOS 6.2.2 product integration and support information:

Web Browsers	• Microsoft Edge 41 • Mozilla Firefox version 59 • Google Chrome version 65 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 41 • Mozilla Firefox version 59 • Google Chrome version 65 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 25. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 25. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 25 and Fortinet Security Fabric upgrade on page 25. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0282 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2008 Core
	  • Novell eDirectory 8.8

FortiExtender	• 3.2.1
AV Engine	• 6.00132
IPS Engine	• 5.00035
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012 R2, and 2016
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network: https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 61 Google Chrome version 68
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 61 Google Chrome version 68
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
OS X El Capitan 10.11.1	Apple Safari version 11 Mozilla Firefox version 61 Google Chrome version 68
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved issues

The following issues have been fixed in version 6.2.2. For inquires about a particular bug, please contact Customer Service & Support.

New features or enhancements

Bug ID	Description
457153	Support for SSL VPN sign on using certificate and remote (LDAP or RADIUS) username/password authentication.
538760	Monitor API to check SLBC cluster checksum status. New API added - monitor/system/config-sync/status.
544704	FortiOS support for 802.11ax FortiAP-U431F/U433F.
550912	Support for link aggregation LACP on entry level FortiGate is extended to all two-digit entry level box for the following models: FGR-30D, FGR-35D, FG-30E, FG-30E-MI, FG-30E-MN, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-POE, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-92D, FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-61E
554965	IPv6 is supported in communication between the following: • Collector agent and FortiGate • Collector agent and DC_agent • Collector agent and terminal server agent

AntiSpam

Bug ID	Description
559802	Spam mail can't be checked by antispam filter on SMTP protocol.

AntiVirus

Bug ID	Description
545381	When `proxy-av` is configured for firewall policy, FTP file upload is stopped.
553143	Redundant logs and alert emails sent when file is sent to FortiSandbox Cloud via *Suspicious Files Only*.
561524	Cannot send an email with PDF attachment when FortiSandbox Cloud Inspection is enabled.
562037	CDR does not disarm files when they are sent over HTTP-POST even though despite AV logs show file has been disarmed.

Bug ID	Description
575177	Advanced Threat Protection Statistics widget clean file count is incorrect.
580212	Policy in flow mode blocking Adobe creative cloud desktop application.

Application Control

Bug ID	Description
558380	`AppCtl` does not detect application with `webproxy-forward-server`.

Data Leak Prevention

Bug ID	Description
522472	DLP logs have a wrong reference link to archived file.
540317	DLP cannot detect attached zip files when receiving emails via MAPI over HTTP.
546964	DLP sensors and DLP options in firewall policy and profile groups are removed.
570379	DLP only detects the first word of filename.

DNS Filter

Bug ID	Description
567172	Enforcing *Safe Search* in 6.0.5 blocks access to Google domains which makes *Safe Search* not work.
578267	DNS request to a second DNS server with same Transaction ID is discarded when DNS Filter is enabled on a policy.
581778	Cannot re-order DNS domain filter list.

Explicit Proxy

Bug ID	Description
543794	High CPU due to WAD process.
552334	Website does not work with SSL Deep inspection due to OCSP validation process.
557265	Browser redirect loop after re-authentication when using `proxy-re-authentication-mode absolute`.
561843	`AppCtl` unscans the traffic to forwarding to upstream proxy.
564582	Explicit proxy policy treats `domain.tld` in FQDN firewall address object as wildcard.
567029	WAD crashes at `crypto_kxp_xform_block_enc` when WAD is restarted while visiting a website after an authentication.

Bug ID	Description
571034	Using disclaimer causes incorrect redirection.
572220	Unable to match the expected firewall proxy-policy when `dstint` is set to Zone where Zone member has PPPoE interface.
577372	WAD has signal 11 crash at `wad_ssl_cert_get_auth_status`.

Firewall

Bug ID	Description
539421	Load Balance monitor stats reset after mode change.
540949	Health status of standby server in server load balance not available in GUI or CLI.
545056	Firewall should not be evaluated when an interface bandwidth widget is added to the dashboard.
552329	NP6 sessions dropped after any change in GUI.
554329	Schedule policy is not activated on time.
558689	Traffic dropped by anti replay in ECMP with IPS.
558690	Session timer left at half-open value once established in an ECMP with IPS context.
563471	HTTP load balancing doesn't work after rebooting in Transparent mode.
563928	SFTP connection failure when SSH DPI and app-ctrl are enabled.
564990	Captive-portal-exempt is not supported in consolidated policy.
566951	Unexpected reverse path check failure on IPv6.
570468	FortiGate randomly not processing some NAT64 packets.
570507	Application control causing NAT hairpin traffic to be dropped. **Workaround**: Create a new firewall policy from scratch and the default application control can be applied again.
571022	SNAT before encryption in policy-based VPN for local traffic after upgrade from 5.6.8 to 6.0.5.
571832	Provide different protocol/port list when the same ISDB object is used as source/destination.
577752	Policy with a VIP with a destination interface of a zone is dropping packets.

FortiView

Bug ID	Description
527540	Cannot click the *Quarantine Host* option on a registered device.
537819	FortiView All Sessions page: tooltip of geography IP show 'undefined'.
553627	FortiView pages cannot load with *Failed to retrieve FortiView data*.

GUI

Bug ID	Description
445074	The MMS profiles pages have been removed from the FortiOS Carrier GUI. **Workaround**: You can configure MMS profiles from the CLI using the `config firewall mms-profile` command.
479692	GUI shows error *Image file doesn't match platform* even when the user is uploading correct image.
486230	GUI on FGT3800D with 5.6.3 is very slow - configuration with numerous policies.
493704	While accessing the FortiGate page, PC browser memory usage keeps spiking and finally PC hangs.
502740	Remove GUI instructions for Dialup-FortiClient VPN.
504829	GUI should not log out if there is 401 error on downstream device.
513157	Cannot filter on hit count "0" for policy match.
523403	GUI Protocol Port Mapping configuration should be rejected when an invalid port number such as *-1* is entered.
526254	Interface page keep loading when VDOM admin have `netgrp` permission.
528649	`vpngrp` read or read-write access profile doesn't work properly.
540056	Error message enhancement while creating packet capture in GUI with filter set to high port range.
540737	Should show warning and block user to use no-inspection SSL-SSH profile when any UTM profile is used.
543487	Collected Email Monitor page cannot list the wireless client if connected from captive-portal+email-collection.
543637	Not able to filter the policy by multiple ID.
544313	GUI SD-WAN Monitor page keep loading.
548653	SSO_admin (super_admin) can't open CLI window from GUI. Error says too many concurrent connection.
552552	*Personal Privacy* in FortiGuard category based filter mistranslated.
555121	Context menu of AP Group has unsupported actions enabled after change view on Managed FortiAPs page.
559799	Webhook automation host header incorrect.
560430	Some app-category cannot be listed on security policy editing page and get JS error.
561334	GUI SSID main passphrase and MPSK minimum length should be flexible according to new "wfa-compatibility" setting.
563053	Warning message for third-party transceivers were removed for 6.2.1 to prevent excessive RMA or support tickets. 6.2.2 re-added the warning for third-party transceivers.
563445	Upgrade NGFW VDOM from v6.2.0, security policy should support virtual-wan-link interface.

Bug ID	Description
564201	After OSPF change via GUI, password for virtual-link will completely disappear and must be re-entered.
564601	Remove the license requirement to upload FortiGuard packages through the GUI when in USG mode.
565109	*Add Selected* button does not appear under *Application Control* slide-in when VDOM is enabled.
566666	AP comments do not appear on the columns for Managed AP page.
568176	GUI response is very slow when accessing Route-Monitor page in GUI.
569080	SD-WAN rule GUI page doesn't show red exclamation mark for DST-negate enabled, like firewall policy.
569259	Fabric SAML with FortiManager management. Downstream FortiGate login with SAML super admin only have read-only access on most pages.
571674	GUI config changes generate misleading config event logs.
571828	GUI admin password injected as PSK when adding phase2 configuration on Chrome.
572027	In Log View/FortiView, GUI cannot list logs from FortiAnalyzer on FGT/FWF boxes.
573070	Interface widget not loading fully (keeps spinning) when a VDOM "prof_admin" is used.
573869	Log search index files are never deleted when the logdisk is out of space.
574239	AWS/AWSONDEMAND missing dropdown selection box for HTTPS server and WiFi certificates in GUI.
575756	Port Link speed option is missing on the FortiGate GUI after upgrading the managed FortiSwitch to 6.2.1.
579259	Firewall User Monitor shows "Failed to retrieve info" and no entries if session-based proxy authentication is used.
583760	After adding few Web Rating Overrides via GUI to an already existing long list of URIs, Web Rating Overrides page is not loaded and keeps spinning.

HA

Bug ID	Description
543602	Unnecessary syncing process started during upgrade when it takes longer.
554187	HA slave gets FW Signature un-certified after upgrading image from the master.
555056	Enable 2-factor using vcluster in GUI gets overwritten (sync) by slave.
555998	Load balanced (A-A) slave-session doesn't forward traffic after session is dirtied due to FortiManager policy install.
557277	FortiGate FGSP configured with standalone-config-sync will sync the FortinAlayzer source-IP configuration to the slave.

Bug ID	Description
557473	FGSP found checksum mismatch after replaced one of the units in the cluster.
559172	VLAN in VDOM in virtual cluster not showing virtual MAC for the vcluster.
560096	Restoring config fails on slave when using TACACS+ (master OK).
560107	Cluster upgrade from 5.6.7 build 1653 to SB 5.6.8 build 3667 takes longer than normal.
563551	HASYNC aborts on slave unit.
569629	HA A-A local FQDN not resolving on slave unit.
574564	In an HA configuration with HA uninterruptible upgrade enabled, some signature database files may fail to synchronize upon upgrading from 5.6.9 and earlier to 5.6.10.
575715	Unable the sync the Local-GW in FGSP.
576638	HA cluster GUI change does not send logs to the slave immediately.
577115	Master unit console keeps showing message `[ha_auth_set_logon_msg:228] buffer overflow`.
578475	FortiGate HA reports not synced if firewall policy of master and slave does not contain the same VIP.

Intrusion Prevention

Bug ID	Description
545823	Creating/editing a DoS-Policy takes a long time. GUI hangs or displays *Error 500: Internal Server Error*.
561623	IPS engine 5.009 crashes when updated new FFDB has different size from the old one.

IPsec VPN

Bug ID	Description
449212	New dialup IPsec tunnel in policy mode/mode-cfg overwrites previously established tunnel.
537450	Site-to-site VPN policy based with DDNS destination fail to connect.
553759	ESP packets are sent to the wrong MAC after a routing change when IPsec SA is offloaded.
558693	FW90D VPN becomes unresponsive after changing VPN DDNS/Monitor.
559180	The command `include-local-lan` gets disabled after firewall is rebooted.
560223	Add support for EdDSA certificates for proxy-based deep-inspection / virtual-server when using TLS 1.3. This is resolved by: 0560223, 0561319, 0561820, 0561821, 0561822, 0561823, 0564510.
564237	After configuring SD-WAN and creating SD-WAN rule based on bandwidth criteria, the bandwidth value for tunnel interface is not calculated correctly.
569586	IPsec certificate based IKEv2 VPNs fail to read out certificate subject as username if ECC certificate is involved.

Bug ID	Description
571209	Traffic over VLAN sub-interface pushed through the IPsec policy based VPN interface.
574115	PKI certificates with OU and/or DC as subject fail for PKI user filters.
575238	Redirected traffic on the same interface (ingress and egress interface are the same) is dropped.
575477	IKED memory leak.
577502	OCVPN cannot register - status 'Undefined'.

Log & Report

Bug ID	Description
387294	Country flags in Botnet C&C table and Top Destinations by Bandwidth table are all missing.
545948	FortiGate periodically stops sending syslog messages.
551459	`srcintf` is `unknown-0` in traffic log for service DNS when action is IP connection error.
556199	No logs are generated when using local-in policy on ha-mgmt interface.
558702	`miglogd` not working until `sysctl killall miglogd`. Reboot does not help.
565216	Memory of `miglogd` increase and enter conserve mode.
565505	`miglogd` high CPU utilization.
566843	No log generated when traffic is blocked by setting `tunnel-non-http` in webproxy.
568795	Specific traffic type is not logged on FAZ/Memory.
576024	Set sniffer policy to only log `logtraffic=utm` but many traffic log stats are still generated in disk or FortiAnalyzer.

Proxy

Bug ID	Description
457347	WAD crashes in `wad_http_client_body_done` when ICAP is enabled.
544414	WAD handles transparent FTP/FTPS traffic.
550056	When SNI is exempt in an SSL profile, and the SNI does not match the CN, the FortiGate closes the session and does not perform deep inspection.
551119	Certificate blacklist not working correctly in proxy mode.
559166	In firmware 6.0.5, WAD CPU usage on all cores reaches 100% in each around 30s.
562610	FortiGate generates WAD crash `wad_mem_malloc`.
563154	Can't open a particular web page via explicit proxy with deep inspection and webfilter profile enabled.
566859	In WAD conserve mode 5.6.8, `max_blocks` value is high on some workers.

Bug ID	Description
567796	WAD constantly crashes every few seconds.
567942	FortiGate cannot block blacklist certificate against TLS 1.3 if the blacklist certificate server address is exempt.
568905	WAD crashes due to RCX null.
572489	SSL handshake sometimes fail due to FortiGate replying back `FIN` to client.
573340	WAD causing memory leak.
573721	For FortiGate with client certificate inspect mode, traffic will trigger WAD crash.
573917	Certain web pages time out.
574171	Fail to connect https://drive.google.com by TLS 1.3.
574730	Wildcard URL filter stops working after upgrade.
576852	WAD process crashes in `internet_svc_entry_cmp`.
581865	In Proxy inspection with Application control and certificate inspection, TLS error for certain web pages,in EDGE browser only.
582714	WAD might leak memory during SSL session ticket resumption.
583736	WAD application crashing in v6.2.1.

REST API

Bug ID	Description
566837	HTTPSD process crashes when using REST API.

Routing

Bug ID	Description
558979	ECMP-based session with auxiliary session and IPS is not offloaded in reply direction.
559645	Creating static route from GUI should set *Dynamic Gateway* disabled by default.
560633	OSPF route for AD-VPN tunnel interface flaps.
562159	ADVPN OSPF unable to ping over ADVPN linknet.
567497	FortiGate sends PIM register messages to RP for group 64.0.0.0 about nonexistent sources.
571714	DHCPv6 relay shows *no route to host* when there are multiple paths to reach it.
573789	OSPF with virtual clustering not learning routes.
578623	Gradual memory increase with full BGP table.
581488	BGP confederation router sending incorrect AS to neighbor-group routers.

SSL VPN

Bug ID	Description
476377	SSL VPN FortiClient login with FAC user FTM two-factor fail because it times out too fast.
478957	SSL VPN web portal login history is not displayed if logs are stored in FortiAnalyzer.
481038	Web application is not loading through SSL VPN portal.
491733	When SSL VPN receives multiple HTTPS post requests under web filter, `read_request_data_f` loops even when client is stopped, which causes the SSL VPN process to use 99% of CPU.
496584	SSL VPN bad password attempt causes excessive bind requests against LDAP and lockout of accounts.
515889	SSL VPN web mode has trouble loading internal web application.
525172	A web application accessed through SSL VPN web mode triggers Error 500 on Java server.
530509	*Invalid HTTP Request* when SMB via SSL VPN bookmark is executed with MS Server 2016, but works fine with MS server 2008R2.
531848	FortiSIEM WebGUI does not load on web portal.
537341	SSL bookmark is not loading SAP portal information.
545177	Web mode fails for SharePoint page.
549654	Citrix bookmarks should be disabled in SSL VPN portal.
549994	SSL VPN web mode logon page should not show *Skip* button for remote user with *Force password change on next logon*.
551695	Office365 applications through SSL VPN bookmarks.
555344	Downloading PDF file throigh SSL VPN portal.
555611	SSL VPN web mode web forward not working for video camera system after upgrade to 6.0.4.
556657	Internal website not working through SSL VPN web mode.
558076	In firmware 6.2.0, RDWeb (Windows Server 2016) via SSL web portal does not work.
558080	McAfee ESM 11 display issues in SSL VPN web portal.
558473	For FG-200E, after upgrading from 6.0.4 to 6.2.0, SSL VPN HTTPS bBookmark does not load (Secure Connection Failed).
559171	With SSL VPN web mode unable to get dropdown menu from internal web page.
559785	FortiMail login page with SSL VPN portal not displaying correctly.
560438	`interface` subnet object not available in SSL VPN `split-tunneling-routing-address`.
560505	SharePoint 2019 page access fails using web mode.
560730	SSL VPN web mode SSO doesn't work for some site like FAc login.
560747	The referer header is not correct, and some files are not loaded properly.

Bug ID	Description
561585	SSL VPN doesn't correctly show Windows Admin center application.
563147	Connection to internal portal freezes when using SSL VPN web bookmark.
563798	Redirect in bookmark is not loading.
564850	Object from CARL source not showing through SSL VPN web mode.
564871	SSL VPN users create multiple connections.
567182	In SSL VPN web mode, videos on internal website won't display.
567626	SSL VPN still allows password expired users to change password and get access.
567628	SSL VPN banned-cipher SHA256 not completely working.
567987	In SSL VPN web mode, RDP disconnects when copying long text from remote to local.
568481	Internal website using java is not accessed using SSL VPN web mode.
568838	Internal website not working through SSL VPN web mode.
569030	SSL VPN tunnel mode can only add split tunneling of user's policy with groups and its users in different SSL VPN policies.
569711	Error for proxy ssh database through SSL VPN.
570445	CMAT application through SSL VPN not working properly.
570620	SSL VPN web mode does not work properly for the website using JavaScript.
571005	NextCloud through SSL VPN behaving strangely.
571479	Cannot access sub-menus from the internal main website through the bookmark when using SSL VPN web mode.
571721	Local portal `adzh-srop-nidm02.intern.cube.ch` needs more than 10 min. to load via SSL VPN bookmark.
572653	Unable to access Qlik Sense URL via SSL VPN web mode .
573527	SSL web portal CSP v3 compatibility issue.
573853	TX packet drops on `ssl.root` interface.
574551	Subpages on internal websites are not working via SSL VPN web mode (Tunnel mode is OK).
574724	SSL VPN conserve mode on FWF-30E when FortiGate unit enters memory less than 25%.
575248	Synology DSM login page is not displayed when accessed via SSL VPN bookmark or connection tool.
575259	SSL VPN connection is being dropped intermittently.
576013	The SSL VPN web mode webserver link is not rewritten correctly after login.
578581	SSL web mode VPN portal freezing when opening some websites using JavaScript.
580182	The EOASIS website is not displayed properly using SSL VPN web mode.

Bug ID	Description
580384	SSL VPN web mode not redirecting URL as expected after successful login.
581863	Accessing http://nlyte.ote.gr/nlyte/ configured with bookmark name 'NLYTE' not getting authentication page.
582115	Third-party (Ultimo) web app does not load over SSL VPN web portal.
582161	Internal web application is not accessable through web SSL VPN.

Switch Controller

Bug ID	Description
557280	Need to add FSW port information on Security Fabric and device inventory the same as before 6.0.4.
563939	802-1X timer `reauth-period` option `0` doesn't work.

System

Bug ID	Description
423311	200E/201E software switch span function does not work.
470875	OID seems to be COUNTER32 instead of GAUGE32.
498599	Can't create loopback interface by VDOM admin if there's no physical interface in VDOM.
520283	Can't show global setting when VDOM admin run `exec tac report` command.
531675	SFP ports do not link down when SFP cat5 interface status of FortiGate on the other side goes down.
539970	Kernel panic on HA pair of 301E.
540083	Partial traffic outage with softirq on 100%.
545449	IPinIP traffic over another IPinIP is dropped in NP6-Lite when offloading is enabled.
550206	Memory (SKB) which is no longer needed is not released in NP6 and NP6lite drivers (100E, 140E, 3600D, 3800D).
551281	`process_tunnel_timeout_notify:377, send timeout notify message error -1 1` message printed in console.
556408	Aggregate link doesn’t work for LACP mode active for 60E internal ports but works for wan1 and wan2 combination.
557172	When there are many application-control based Internet-service entries in SD-WAN, system performance is affected by high CPU usage of softirq.
557527	FortiGate as L2TP client does not negotiate correctly.
557798	High memory utilization caused by `authd` and WAD processes.

Bug ID	Description
559467	Support four DNS records inside DHCP offer.
560411	3980E unresponsive with millions of sessions in TIME_WAIT.
560686	4x10G split-port does not work on FG-3700D rev 2.
561097	SD-WAN rule corrupted on reboot after ISDB update.
561234	FG-800D shows wrong HA, ALERM LED status.
561929	REST API `cmdb/router/aspath-list` is not inserting new values.
562049	TLS 1.3 resumption and Pre-Shared Key (PSK) fail if Hello Retry Request is received.
563232	Authorization fails when 0.0.0.0/0 is listed as the trusted host.
563497	The `trust-ip-x` feature on interface does not work.
564184	Split DNS not working. CNAME fails to resolve.
564579	Updated crash signal 14, object creation not allowed from cli errno=Resource temporarily unavailable.
564911	DHCPDISCOVERY NATed with TP management IP when sent to NAT VDOM .
565291	SD-WAN rule doesn't work with nested firewall address group selected as source or destination.
565296	Wrong configuration transmitted by FOS to FortiManager under certain conditions.
565631	DHCP relay sessions are removed from the session table after applying any config change.
567487	CPU goes to 100% when modifying members of an `addrgrp` object.
567504	Speed test break the cluster.
568215	Kernel bug at net/core/skbuff.
569652	High memory utilization after FortiOS and IPSengine upgrade.
570227	FortiGate is not selecting an NTP server that has a clock time in the majority clique of other NTP servers.
570575	PoE ports no longer deliver power.
570834	STP (Spanning Tree) flapping.
571207	DHCP with manual address does not provide subnetmask in DHCP ACK.
572411	Timezone for Canary Islands is missing.
572428	lldptx - Application Crashed - Signal 11 Segmentation Fault.
572707	Configuration is corrupted when restoring a VDOM.
572763	softirq causing high CPU when session increase in an acceptable way.
573177	GUI cannot save edits made on replacement messages in a VDOM. When using CLI, user gets logged out while editing.

Bug ID	Description
574086	Kernel panic occurs after upgrading from 6.2.0 to 6.2.1.
574110	When adding admin down interface as a member of aggregate interface, it shows up and process the traffic.
574327	FortiGate CSR traffic to SCEP srv generated from the root VDOM instead of the VDOM we create the CSR.
574991	FortiGate can't extract the user principal name `UPN` from user certificate when certificate contains UPN and additional names.
576063	Crashlog keeps having `cid could not load sigs` after FortiGate is authed into FortiManager.
577047	FortiGate takes a long time to reboot when it has many firewall addresses used in many policies.
577302	Virtual WAN Link process (vwl) memory usage keeps increasing after upgrading to 6.2.1.
578531	`forticldd` deamon resolved `mgrctrl1.fortinet.com` to wrong IP address.
578746	FortiGate does not accept FortiManager created country code and causes address install fails.
579524	DHCP lease is not stable and `dhcpd` process crashes.
580185	`authd4` crashes when deleting a VDOM or rebooting the FortiGate.
580883	DNS servers acquired via PPPoE in non-management VDOMs are used for DHCP DNS server option 6.
582547	`fgfmsd` crash makes connection to FortiManager go down.

Upgrade

Bug ID	Description
550410	Cannot edit `addrgrp` which includes `wildcardfqdn` object after upgrade from v5.6.x.
556002	Some firewall policies were deleted after upgrade from FOS 6.0.4 to FOS 6.2.0.
558995	L2 WCCP stops working after upgrade to FOS 6.0.3 or newer.
562444	The firewall policy with internet-service enabled was lost after upgrade from 6.0.5.
580450	Policies removed after an upgrade in NGFW Policy Mode: maximum number of entries has been reached.

User & Device

Bug ID	Description
547657	Disclaimer+Auth Guest portal RADIUS auth failing due to FAC trying to resolve 3rd party websites as access-points.
549394	`fnbamd` crashes frequently.

Bug ID	Description
558332	CoA from FAC is not working for FortiGate wired interface based captive portal.
561289	User-based Kerberos Authentication not working in new VDOM.
561610	`src-vis` process memory leak.
562185	Disclaimer redirection to IP instead of FQDN results in Certificate/SSL warning.
562861	RADIUS CoA (disconnect request) not working with `use-management-vdom`.
567990	Hard-timeout setting not working for captive portal.

VM

Bug ID	Description
524052	Application `cloudinitd` has signal 11 crash on FortiGate-VM64-GCP.
561083	VPN tunnels not coming up after HA failover in GCP.
561909	Azure SDN connector try querying invalid FQDN when using Azure Stack Integrated systems.
567137	VM in Oracle cloud has 100% CPU usage in system space.
570176	HA cluster multi AZ does not failover IPsec VPN in AWS with TGW.
571652	OCI SDN connector gets `HTTP response err:500` when enabling `use-metadata-iam`.
573952	FGT-VM with network driver vmxnet3 has lots of fragments when testing throughput.
575400	In Azure SDN, the firewall address filter cannot fetch the secondary public and private IP addresses of the NICs.
578727	FGTVM_OPC unable to failover the route properly during failover.
578966	OpenStack PCI passthru sub interface VLAN cannot received traffic.
580738	In the Cluster setup, slave unit can have different fingerprint for the OCI SDN connector, which can cause unit to fail to connect to OCI metatdata server properly.
580911	EIP assigned to the secondary IP address on the OCI do not 't fail over during HA failover.
577856	Add missing AWS HA failover error log and set firewall.vip/vip46/vip6/vip64 not sync'ing when cross zone HA is configured.

VoIP

Bug ID	Description
570430	SIP ALG generates a VoIP session with wrong direction.
580588	SDP information fields are not being natted in Multipart Media Encapsulation traffic.

WanOpt

Bug ID	Description
564290	FOS can't collaborate web-cache with FortiProxy successfully.

Web Filter

Bug ID	Description
356487	When central-management is `NONE`, `include-default-servers` setting is not honored by rating.
549928	Block page images not loading for web sites protected by HSTS.
551956	Proxy web filtering blocks innocent sites due to `urlsource="FortiSandBox Block"`.
565952	Proxy-based Webfilter breaks WCCP traffic.

WiFi Controller

Bug ID	Description
540027	FortiWiFi working as client mode cannot see and connect to the hotspot SSID from iOS devices.
569966	WPA2-Enterprise SSID authentication cannot utilize the source IP setting in RADIUS server configuration.
570745	FAPs detecting BSSIDs of others FAPs managed by the same WC as `Fake-ap-on-air`.
573024	FAP cannot be managed by FortiGate when admin trusthost is configured.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
569310	FortiOS 6.2.2 is no longer vulnerable to the following CVE Reference: • CVE-2019-15703

Known issues

The following issues have been identified in version 6.2.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Data Leak Prevention

Bug ID	Description
586689	Downloading a file with FTP client in EPSV mode will hang.

DNS Filter

Bug ID	Description
586526	Unable to change DNS filter profile category action after upgrading from 6.0.5 to 6.2.0.

FortiView

Bug ID	Description
582341	Fortiview > policies: Consolidate policy without name and tooltips, Security policy with tooltips are not working.

GUI

Bug ID	Description
282160	GUI does not show byte info for aggregate and VLAN interface.
438298	When VDOM is enabled, the interface faceplate should only show data for interfaces managed by the admin.
480731	Interface filter get incorrect result (EMAC VLAN, VLAN ID, etc.) when entries are collapsed.
510685	Hardware Switch Row is shown, indicating a number of interfaces but without any interfaces below.
514632	Inconsistent `Refcnt` value in GUI when using ports in HA `session-sync-dev`.
535099	GUI should add support for new MAC address filter in SSID dialog page.
537307	Gets "Fail to retrieve info" for `ha-mgmt-interface` on GUI > interface page.
540098	GUI does not display the status for VLAN and loopback under status column at Network > interfaces.
541042	Log viewer Forward Traffic cannot support double negate filter (client side issue).
542544	In Log & Report, filtering for blank values (None) always show no results.

Bug ID	Description
553290	The tooltip of VLAN interface displays *Failed to retrieve info* on GUI.
557786	GUI response is very slow when accessing IPSec-Monitor (api/v2/monitor/vpn/ipsec is taking a long time).
559866	When sending CSF proxied request, `segfault` happens (`httpsd` crashes) if FortiExplorer accesses root FortiGate via management tunnel.
565748	New interface pair consolidated policy added via CLI is not displayed on GUI policy page.
573456	FortiGate without disk *Email Alert Settings* page should remove *Disk usage exceeds* option.
574101	Empty firmware version in managed FortiSwitch from FortiGate GUI.
579711	An error occurs while running Security Rating.
583049	Internal Server Error while trying to create new interface.
584939	VPN event logs shows incorrectly when adding two action filters and if the filter action filter contains "-".
586604	No matching IPS signatures are found when the Severity or Target filters are applied.
586749	Enable/Disable *Disarm and Reconstruction* on GUI only takes effect on SMTP protocol in AV profile.

HA

Bug ID	Description
479780	Slave fails to send and receive HA heartbeat on `config cfg-revert` setting on FGT2500E.
575020	HA failing config sync on VM01 with error (slave and master have different hdisk status) when master is pre-configured.
581906	HA slave sending out GARP packets in 16-20 seconds after HA monitored interface failed.
586004	Moving VDOM via GUI between virtual clusters causes cluster to go out of sync but VDOM state work/standby doesn't change.
588908	FG-3400E `hasync` reports the "Network is unreachable".

IPsec VPN

Bug ID	Description
582251	IKEv2 with `eap auth peerid` validation doesn't work.

Proxy

Bug ID	Description
573028	WAD crashes causing traffic interruption.
575224	WAD - high memory usage from worker process causing conserve mode and traffic issues.

REST API

Bug ID	Description
584631	REST API admin with token unable to configure HA setting (via login session can work).

Security Fabric

Bug ID	Description
578268	Downstream device shows offline.
586587	Security Fabric widget keep loading when FortiSwitch is in a loop or two FortiSwitches are in `mclag` mode.
587758	Invalid CIDR format shows as valid by Security Fabric threat feed.
588262	IP address threat feed fabric connector not working.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.
563022	SSL VPN LDAP group object matching only matches the first policy, isn't 't consistent with normal firewall policy.
585754	An SSL VPN bookmark failed to load the GUI of `proxmox` GUI interface.

Switch Controller

Bug ID	Description
581370	FortiSwitch managed by FortiGate not updating RADIUS settings and user group in the FortiSwitch.
586299	Adding factory-reset device to HA fails with `switch-controller.qos` settings in root.

System

Bug ID	Description
464340	EHP drops for units with no NP_SERVICE_MODULE.
484749	TCP traffic with `tcp_ecn` tag cannot go through ipip IPv6 tunnel with NP6 offload enabled.
555616	TCP packets send wrong interface and high CPU.
562212	Management tunnel to devices goes down and cannot reclaim tunnel; so policy pushes get stuck.
570759	RX/TX counters for VLAN interfaces based on LACP interface are 0.

Bug ID	Description
573973	ASIC offloading sessions sticking to interfaces after SD-WAN SLA interface selection.
575013	Errors in the FortiGate's CLI 8 debug, when FortiManager is obtaining the HA status and `mgmt-data` status, if `ha-mgmt-status enabled`.
581998	Session clash event log found on FG-6500F when passing a lot of same source IP ICMP traffic over Load balance VIP.
586301	GUI cannot show default Fortinet logo for replacement messages.
589234	`system local dns` instead of DNS setting acquired from upstream DHCP server was assigned to client under `management-vdom`.

User & Device

Bug ID	Description
569062	`fnbamd` takes high CPU usage and user cannot authenticate.

VM

Bug ID	Description
579013	FortiGate HA failover fails in Azure stack due to invalid authentication token tenant.
579708	Should replace GUI option to register to FortiCare from AWS PAYG with link to portal for registration.
587180	FGTVM64_KVM is unable to boot up properly when doing a hard reboot with the host.
587757	FG-VM image unable to be deployed on AWS with additional disk of type HDD(st1).
588436	Azure SDN connector unable to connect to Azure Kubernetes integrated with AAD.

WiFi Controller

Bug ID	Description
555659	When FAP is managed across VDOM links, WiFi client can't join SSID when `auto-asic-offload` is enabled.
572350	FortiOS GUI cannot support FAP-U431F and FAP-U433F profiles. **Workaround**: Edit the `wtp-profile` for FAP-U431F and FAP-U433F in the CLI.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.